

Abstract

This patent describes a data processing system and method for performing mutual authentications between two security tokens by generation of a common cryptographic key. The common cryptographic key is generated using unique identifiers associated with each security token that diversify a common master key. The generation process incorporates a message digest function such as SHA-1 and an XOR operator to arrive at the common symmetric key.

20061014E285001